EXHIBIT 1

Blog > Unimania: I Need Your Facebook Data, Location, And Your Browsing History

Unimania: I Need Your Facebook Data, Location, And Your Browsing History

Privacy protection is basically what we do, so I never get tired of stories about how unpredictable the ways of getting Facebook user data are. Cambridge Analytica might be dead, but the business of stealing users' data lives on, and this article demonstrates one more example of that.

The story begins with the recent research I conducted about fake ad blockers in the Chrome Web Store. The outcome of that research was that I received dozens of questions about whether this or that extension is safe to use. This made me take a deeper look into the most popular Chrome extensions, but even so, I had no idea at that time where this investigation was going to lead me. In fact, it exposed to me a huge spyware campaign that utilizes popular Android apps and Chrome extensions to steal Facebook data and the browsing histories of millions of users.

Suspicious Chrome extensions

I conducted an automated scan of all publicly available Chrome extensions. This scan flagged quite a few different privacy issues, which I will address in more specific detail in a forthcoming post.

One of the issues that immediately caught my attention, as I noticed suspicious requests made to various Facebook domains.

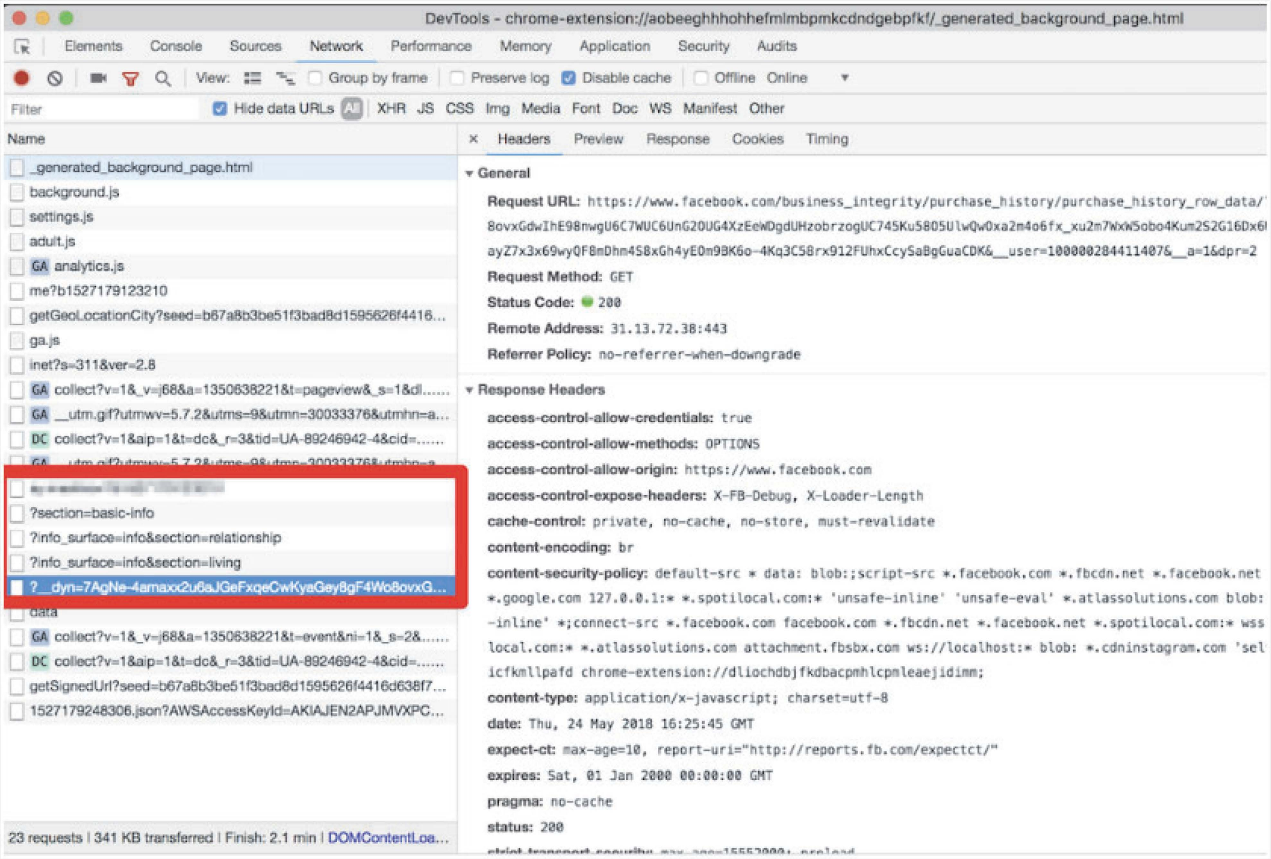
Meet these nasty Chrome extensions, currently in use by an estimated 420,000 users:

- Video Downloader For Facebook (170K+ users, archived copy)
- Album & Photo Manager For Facebook (92K+ users, archived copy)
- PDF Merge - PDF Files Merger (125K+ users, archived copy)
- Pixcam - Webcam Effects (31K+ users, archived copy)

So, what is wrong with them? Let's dive into the details.

The inscrutable ways of your Facebook data

If you are logged into Facebook, these spyware extensions will scrape all your data immediately after the browser startup:


DevTools - chrome-extension://aobeeghhhohhefmlmbpmkcdndgebpfkf/_generated_background_page.html
Elements Console Sources Network Performance Memory Application Security Audits
View: □ Group by frame □ Preserve log ☑ Disable cache □ Offline Online ▾
Filter ☑ Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other
Name
× Headers Preview Response Cookies Timing

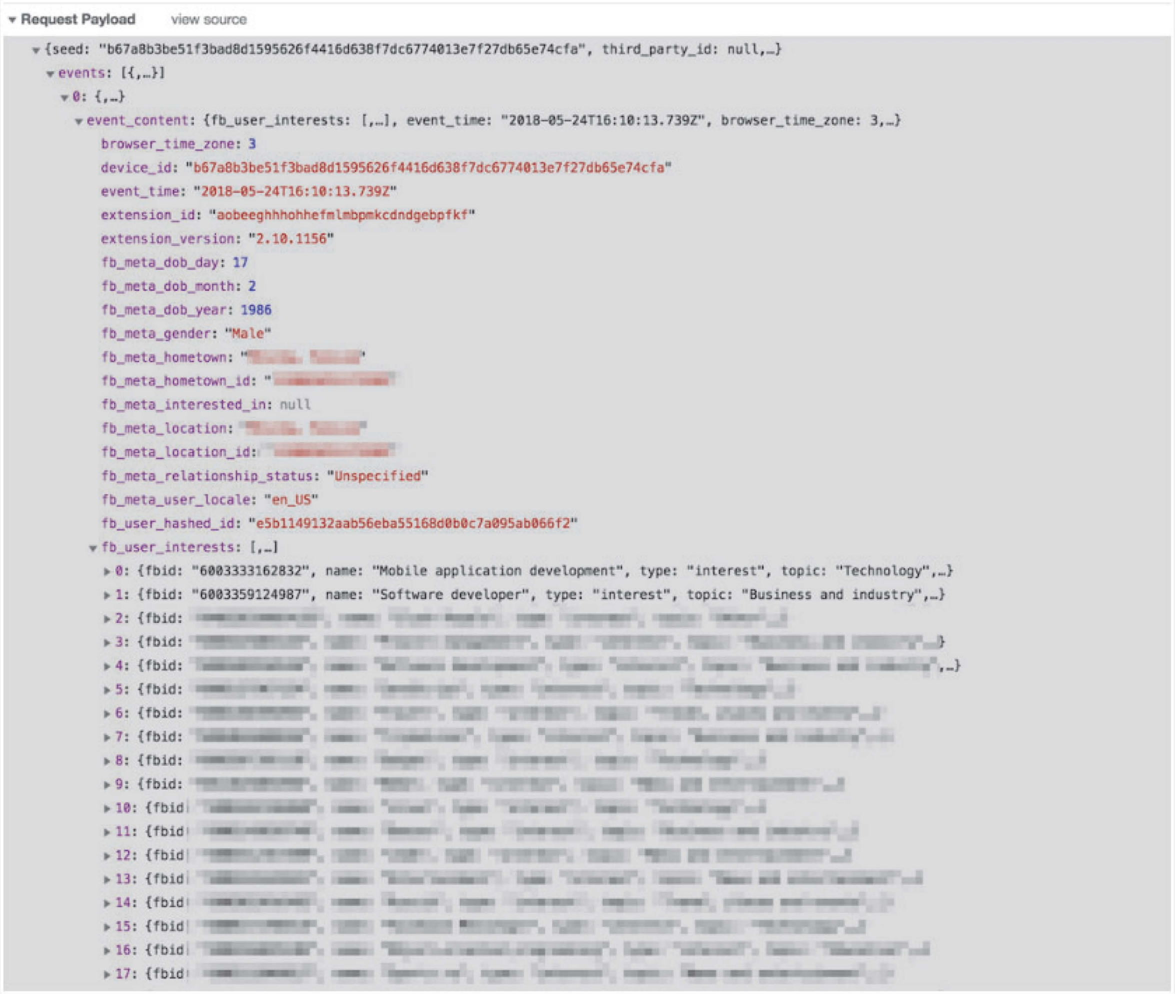
```
_generated_background_page.html
background.js
settings.js
adult.js
GA analytics.js
me?b1527179123210
getGeoLocationCity?seed=b67a8b3be51f3bad8d1595626f4416...
ga.js
inet?s=311&ver=2.8
GA collect?v=1&_v=j68&a=1350638221&t=pageview&_s=1&dl......
GA __utm.gif?utmwv=5.7.2&utms=9&utmn=30033376&utmhn=a...
DC collect?v=1&aip=1&t=dc&_r=3&tid=UA-89246942-4&cid=......
GA __utm.gif?utmwv=5.7.2&utms=9&utmn=30033376&utmhn=a
[redacted]
?section=basic-info
?info_surface=info&section=relationship
?info_surface=info&section=living
?__dyn=7AgNe-4amaxx2u6aJGeFxqeCwKyaGey8gF4Wo8ovxG...
data
GA collect?v=1&_v=j68&a=1350638221&t=event&ni=1&_s=2&......
DC collect?v=1&aip=1&t=dc&_r=3&tid=UA-89246942-4&cid=......
getSignedUrl?seed=b67a8b3be51f3bad8d1595626f4416d638f7...
1527179248306.json?AWSAccessKeyId=AKIAJEN2APJMVXPC...

23 requests | 341 KB transferred | Finish: 2.1 min | DOMContentLoa...
```

```
▼ General
   Request URL: https://www.facebook.com/business_integrity/purchase_history/purchase_history_row_data/'
   8ovxGdwIhE98nwgU6C7WUC6UnG20UG4XzEeWDgdUHzobrzogUC745Ku5805UlwQw0xa2m4o6fx_xu2m7WxW5obo4Kum2S2G16Dx6
   ayZ7x3x69wyQF8mDhm458xGh4yE0m9BK6o-4Kq3C58rx912FUhxCcySaBgGuaCDK&__user=10000284411407&__a=1&dpr=2
   Request Method: GET
   Status Code: ● 200
   Remote Address: 31.13.72.38:443
   Referrer Policy: no-referrer-when-downgrade
▼ Response Headers
   access-control-allow-credentials: true
   access-control-allow-methods: OPTIONS
   access-control-allow-origin: https://www.facebook.com
   access-control-expose-headers: X-FB-Debug, X-Loader-Length
   cache-control: private, no-cache, no-store, must-revalidate
   content-encoding: br
   content-security-policy: default-src * data: blob:;script-src *.facebook.com *.fbcdn.net *.facebook.net
   *.google.com 127.0.0.1:* *.spotilocal.com:* 'unsafe-inline' 'unsafe-eval' *.atlassolutions.com blob:
   -inline' *;connect-src *.facebook.com facebook.com *.fbcdn.net *.facebook.net *.spotilocal.com:* wss
   local.com:* *.atlassolutions.com attachment.fbsbx.com ws://localhost:* blob: *.cdninstagram.com 'sel
   icfkmllpafd chrome-extension://dliochdbjfkdbacpmhlcpmleaejidimm;
   content-type: application/x-javascript; charset=utf-8
   date: Thu, 24 May 2018 16:25:45 GMT
   expect-ct: max-age=10, report-uri="http://reports.fb.com/expectct/"
   expires: Sat, 01 Jan 2000 00:00:00 GMT
   pragma: no-cache
   status: 200
   strict-transport-security: max-age=15552000; preload
```

They even try to parse your purchase history! This alone is enough for these extensions to be booted from the Chrome Web Store.

All this data is then collected and sent to the `um-public-panel-prod.s3.amazonaws.com` domain, which is a named Amazon S3 instance rented by the spyware authors.



```
▾ {seed: "b67a8b3be51f3bad8d1595626f4416d638f7dc6774013e7f27db65e74cfa", third_party_id: null,…}
  ▾ events: [{,…}]
    ▾ 0: {,…}
      ▾ event_content: {fb_user_interests: [,…], event_time: "2018-05-24T16:10:13.739Z", browser_time_zone: 3,…}
          browser_time_zone: 3
          device_id: "b67a8b3be51f3bad8d1595626f4416d638f7dc6774013e7f27db65e74cfa"
          event_time: "2018-05-24T16:10:13.739Z"
          extension_id: "aobeeghhhohhefmlmbpmkcdndgebpfkf"
          extension_version: "2.10.1156"
          fb_meta_dob_day: 17
          fb_meta_dob_month: 2
          fb_meta_dob_year: 1986
          fb_meta_gender: "Male"
          fb_meta_hometown: "[redacted]"
          fb_meta_hometown_id: "[redacted]
          fb_meta_interested_in: null
          fb_meta_location: [redacted]
          fb_meta_location_id: [redacted]
          fb_meta_relationship_status: "Unspecified"
          fb_meta_user_locale: "en_US"
          fb_user_hashed_id: "e5b1149132aab56eba55168d0b0c7a095ab066f2"
        ▾ fb_user_interests: [,…]
          ▸ 0: {fbid: "6003333162832", name: "Mobile application development", type: "interest", topic: "Technology",…}
          ▸ 1: {fbid: "6003359124987", name: "Software developer", type: "interest", topic: "Business and industry",…}
          ▸ 2: {fbid: [redacted]
          ▸ 3: {fbid: [redacted]
          ▸ 4: {fbid: [redacted]
          ▸ 5: {fbid: [redacted]
          ▸ 6: {fbid: [redacted]
          ▸ 7: {fbid: [redacted]
          ▸ 8: {fbid: [redacted]
          ▸ 9: {fbid: [redacted]
          ▸ 10: {fbid[redacted]
          ▸ 11: {fbid[redacted]
          ▸ 12: {fbid[redacted]
          ▸ 13: {fbid[redacted]
          ▸ 14: {fbid[redacted]
          ▸ 15: {fbid[redacted]
          ▸ 16: {fbid[redacted]
          ▸ 17: {fbid[redacted]
```

An alarming amount of data was being sent over to that server including all the Facebook "interests". In order to test this, I had to use my own account, so you can observe a piece of my own data, which I don't mind sharing with you.

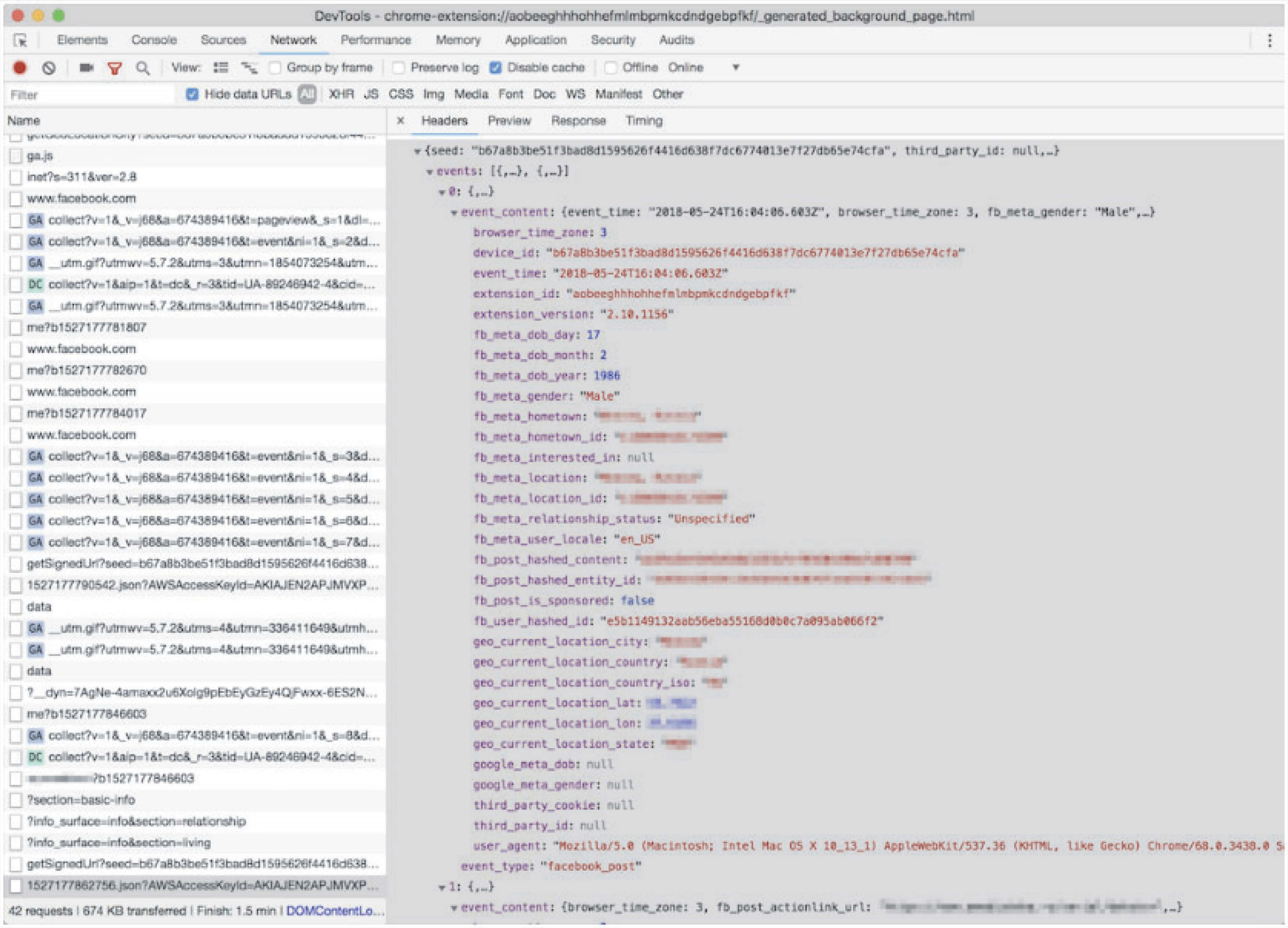
As you can see on the screenshot, they do not send a plain FB identifier; instead, they send it in a hashed form. I imagine that they think that this practice allow the spyware group to say that this data has been made "anonymous."

> “Dear spyware developers, come on! Do you really believe that hashing a numeric value with a static salt cannot be decoded?”

```
SHA1("sME9Azj8G28Y" + userId) = e5b1149132aab56eba55168d0b0c7a095ab066f2
```

> By the way, dear reader, here is a contest for you: the first one to crack the hash and discover my FB ID gets a free AdGuard license. Write your answer in the comments. No cheating, please :)

But hey, what is the good of having this data without the spyware company also knowing what exactly you do on the Internet? Wouldn't it be so much better if they knew what exact posts you read or what exact ads you see? Well, no worries, that's exactly what they do: they siphon information about all of the posts, sponsored posts, tweets, the YouTube videos and ads you see or interact with, along with a poorly hashed user ID and totally UN-hashed location data.



□ Group by frame □ Preserve log ☑ Disable cache □ Offline

☑ Hide data URLs

```
ga.js
inet?s=311&ver=2.8
www.facebook.com
GA collect?v=1&_v=j68&a=674389416&t=pageview&_s=1&dl=...
GA collect?v=1&_v=j68&a=674389416&t=event&ni=1&_s=2&d...
GA __utm.gif?utmwv=5.7.2&utms=3&utmn=1854073254&utm...
DC collect?v=1&aip=1&t=dc&_r=3&tid=UA-89246942-4&cid=...
GA __utm.gif?utmwv=5.7.2&utms=3&utmn=1854073254&utm...
me?b1527177781807
www.facebook.com
me?b1527177782670
www.facebook.com
me?b1527177784017
www.facebook.com
GA collect?v=1&_v=j68&a=674389416&t=event&ni=1&_s=3&d...
GA collect?v=1&_v=j68&a=674389416&t=event&ni=1&_s=4&d...
GA collect?v=1&_v=j68&a=674389416&t=event&ni=1&_s=5&d...
GA collect?v=1&_v=j68&a=674389416&t=event&ni=1&_s=6&d...
GA collect?v=1&_v=j68&a=674389416&t=event&ni=1&_s=7&d...
getSignedUrl?seed=b67a8b3be51f3bad8d1595626f4416d638...
1527177790542.json?AWSAccessKeyId=AKIAJEN2APJMVXP...
data
GA __utm.gif?utmwv=5.7.2&utms=4&utmn=336411649&utmh...
GA __utm.gif?utmwv=5.7.2&utms=4&utmn=336411649&utmh...
data
?__dyn=7AgNe-4amaxx2u6Xolg9pEbEyGzEy4QjFwxx-6ES2N...
me?b1527177846603
GA collect?v=1&_v=j68&a=674389416&t=event&ni=1&_s=8&d...
DC collect?v=1&aip=1&t=dc&_r=3&tid=UA-89246942-4&cid=...
[redacted]?b1527177846603
?section=basic-info
?info_surface=info&section=relationship
?info_surface=info&section=living
getSignedUrl?seed=b67a8b3be51f3bad8d1595626f4416d638...
1527177862756.json?AWSAccessKeyId=AKIAJEN2APJMVXP...
42 requests | 674 KB transferred | Finish: 1.5 min | DOMContentLo...
```

```
▾{seed: "b67a8b3be51f3bad8d1595626f4416d638f7dc6774013e7f27db65e74cfa", third_party_id: null,…}
  ▾events: [{,…}, {,…}]
    ▾0: {,…}
      ▾event_content: {event_time: "2018-05-24T16:04:06.603Z", browser_time_zone: 3, fb_meta_gender: "Male",…}
          browser_time_zone: 3
          device_id: "b67a8b3be51f3bad8d1595626f4416d638f7dc6774013e7f27db65e74cfa"
          event_time: "2018-05-24T16:04:06.603Z"
          extension_id: "aobeeghhhohhefmlmbpmkcdndgebpfkf"
          extension_version: "2.10.1156"
          fb_meta_dob_day: 17
          fb_meta_dob_month: 2
          fb_meta_dob_year: 1986
          fb_meta_gender: "Male"
          fb_meta_hometown: [redacted]
          fb_meta_hometown_id: [redacted]
          fb_meta_interested_in: null
          fb_meta_location: [redacted]
          fb_meta_location_id: [redacted]
          fb_meta_relationship_status: "Unspecified"
          fb_meta_user_locale: "en_US"
          fb_post_hashed_content: [redacted]
          fb_post_hashed_entity_id: [redacted]
          fb_post_is_sponsored: false
          fb_user_hashed_id: "e5b1149132aab56eba55168d0b0c7a095ab066f2"
          geo_current_location_city: [redacted]
          geo_current_location_country: [redacted]
          geo_current_location_country_iso: [redacted]
          geo_current_location_lat: [redacted]
          geo_current_location_lon: [redacted]
          geo_current_location_state: [redacted]
          google_meta_dob: null
          google_meta_gender: null
          third_party_cookie: null
          third_party_id: null
          user_agent: "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3438.0 S
        event_type: "facebook_post"
    ▾1: {,…}
      ▾event_content: {browser_time_zone: 3, fb_post_actionlink_url: [redacted],…}
```

Meet Unimania Inc.

Who is behind this activity? The only thing I knew about the authors was the link to their extensions' privacy policy: `http://privacy.unimania.xyz/privacy_policy.pdf` (here's a copy, just in case). As usual, there's a lot of confusing legalese about how you provide them with consent without doing anything, how seriously they care about your privacy, how strongly your data is made (or kept) anonymous and how it can in no way can be traced back to you as it is protected by a powerful mathematical "hash function."

Fortunately, it is also pretty transparent about what exact information about you is collected:

> **What Information We Collect and How We Collect It**. In general, the Information we collect includes nonpersonally identifiable demographic and psychographic data as well as sponsored campaigns, advertisements or posts that target you directly or that have been shared with you.

Also, I found their EULA (copy) from which I learned that the company name is "Unimania, Inc." and they claim to be located in Tel-Aviv, Israel. However, I could not find any information on this company in the Israeli company register.

My story might have ended here, but there was a sentence in the privacy policy that caught my attention:

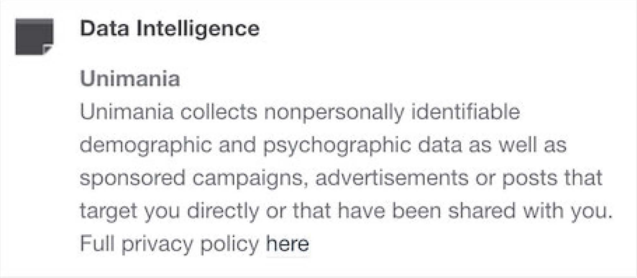
> **Background.** You have been directed to this Privacy Policy from a separate and independent third party Google Chrome Extension or Mobile Software Application (“Third Party Software”).

Mobile Software Application

"Mobile Software Application!" I said to myself.

So this was not just a matter limited to Chrome extensions, and I realized that I needed to continue my investigation. To this end, some good news was that we already had some data collected while preparing a study on mobile apps tracking and I could make use of it and query it right away.

That's how I found one particular app that was connecting to the Unimania servers. This was an alternative Facebook client called "Fast - Social App" with a record of more than 10,000,000 installs according to Google Play. The app developer does not bother to hide that fact and mentions Unimania in the privacy policy:



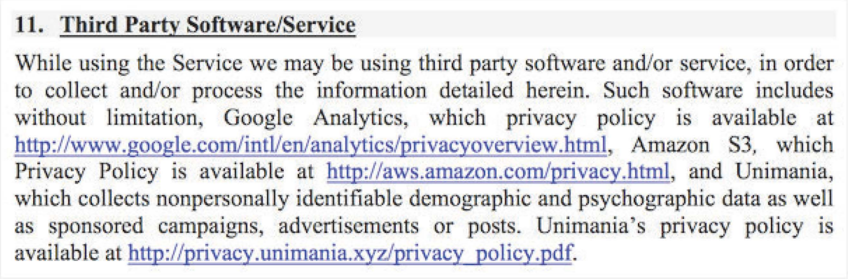
Data Intelligence

Unimania
Unimania collects nonpersonally identifiable demographic and psychographic data as well as sponsored campaigns, advertisements or posts that target you directly or that have been shared with you. Full privacy policy here

Scanning this developer apps' traffic confirmed that "Fast-Social App" transfers pretty much the same data as the Chrome extensions do, and to the same Unimania servers. I also found out that "Fast Lite - Social App + Twitter" (1,000,000+ installs) also does the same thing.

Besides that, I found a couple more apps that mention Unimania in their privacy policies. I cannot confirm that they are still leaking user data, but I can assume they were doing so in the past; otherwise, why would they mention it?

- PhotoMania - Photo Effects (1,000,000+ installs, policy).
- All In One Social Media "Fast" (100,000+ installs, policy)



11. Third Party Software/Service

While using the Service we may be using third party software and/or service, in order to collect and/or process the information detailed herein. Such software includes without limitation, Google Analytics, which privacy policy is available at http://www.google.com/intl/en/analytics/privacyoverview.html, Amazon S3, which Privacy Policy is available at http://aws.amazon.com/privacy.html, and Unimania, which collects nonpersonally identifiable demographic and psychographic data as well as sponsored campaigns, advertisements or posts. Unimania's privacy policy is available at http://privacy.unimania.xyz/privacy_policy.pdf.

Finally, it seems that Unimania is about to launch their own "products":

- OmniSocial - a mobile app
- Who's following me? - a browser extension

Obviously, none of these apps describe this behavior in the app description; neither do they have an "in-app disclosure" as required by Google. I must admit that the Google Play Developer Policies look solid, and so they are likely not the reason of why the privacy of Android apps is in such a sad state. The problem is that these policies are **not enforced**, hence most of the app developers simply ignore them.

Summary

Congratulations for reading through such a long article (or for skipping all the boring technical details and jumping straight to the summary)!

Let's summarize what we discovered.

1. A huge spyware campaign engaging some Mobile Apps and Chrome extensions in stealing users' Facebook data and spying on their social network browsing history. The list of the information collected by these apps and extensions includes the user's Facebook profile data including demographics and the list of user interests. Also, they were collecting the users' browsing history including all the Facebook regular and sponsored posts, tweets, YouTube videos and ads.
2. Four spyware Chrome extensions with aggegrated users count of more than 400,000 users.
3. Two Android apps with total installs count of more than 11,000,000 selling out their users data.
4. The campaign is run by a supposed Israeli company named "Unimania, Inc." Unfortunately, I was not able to trace this further back to Unimania's owners or affiliates and I can't say who is profiting from the data.

I've reported all the discovered apps and extensions to Google and I hope they take corrective measures soon.

How to protect yourself?

The answer to this question is both very simple and very difficult.

When installing anything on your device or browser, follow these rules:

- Read the privacy policy. It is not useless - everything discovered in this case was mentioned in the privacy policies.
- **Never ever install anything made by a developer you don't trust**. Do your homework, find out who the developer is and decide for yourself if they are trustworthy.

Also, all Unimania domains have now been added to the "AdGuard Spyware filter" and will be blocked automatically if you have it enabled in any of our AdGuard products, or if you use AdGuard DNS. Unfortunately, there is a browser limitation that prevents an extension from controlling requests made by other extensions so using the AdGuard Chrome extension or uBlock Origin may not be enough, even if you have the "AdGuard Spyware filter" enabled.

Alternatively, you can block these three domains by adding them to the "hosts" file:

- `um-public-panel-prod.s3.amazonaws.com`
- `collection-endpoint-prod.herokuapp.com`
- `collection-endpoint-staging.herokuapp.com`

UPD (Jun 3): The Android apps mentioned in the article are no more available on Google Play.
UPD (Jun 5): The Chrome extensions are finally taken down from the Chrome Web Store.

Andrey Meshkov on AdGuard Research, Industry News

MAY 30, 2018

Show a site map

Page URL: https://adguard.com/en/blog/unimania-spyware-campaign.html